Лабораторна робота № 3.

Виконали: студенти групи ФІ32мн Ємець Єлизавета
Карловський Володимир
Коваленко Дар'я

Тема: "Дослідження криптографічних протоколів систем WebMoney, PayPal".

Мета роботи: "Дослідження особливостей реалізації криптографічних механізмів платіжних систем".

Завдання на лабораторну роботу

Група 1. Дослідити особливості реалізації криптографічних протоколів, а також особливості роботи з електронними гаманцями систем WebMoney та PayPal. Звіт має містити детальний опис проведеного дослідження особливостей реалізації криптографічних механізмів протоколів систем WebMoney та PayPal. Також звіт має містити загальні теоретичні відомості побудови платіжних систем та їх основні характеристики (специфікація SET), зокрема систем мікроплатежів, таких як Payword та Micromint, та протоколи електронних грошей. Для кожної наведеної системи або протоколу необхідно обґрунтувати його захищеність та вибір криптографічних примітивів.

1. **Вступ**
    - Огляд платіжних систем: поняття, мета та значення захищеності.

    Платіжна система - це набір правил, процедур, технічних засобів та організацій, що забезпечують здійснення грошових переказів між учасниками економічних відносин.

    Учасники системи: Банки та фінансові установи, Торговці, Користувачі, Процесингові центри, Регулятори

    Мета: Забезпечення розрахунків, Зниження фінансових ризиків, Підвищення ефективності грошового обігу, Стимулювання економічного розвитку.

Значення захищеності: Захист від шахрайства та кіберзагроз, Забезпечення конфіденційності даних користувачів, Гарантування цілісності транзакцій.

- Роль криптографічних протоколів у сучасних електронних платіжних системах.

  Криптографічні протоколи в електронних платіжних системах відіграють критичну роль у забезпеченні безпеки транзакцій. Найбільш використовувані: SSL/TLS, який створює захищений канал зв'язку між клієнтом і сервером.

  Але нас більше цікавлять протоколи процесингу платежів: EMV (Europay, Mastercard і Visa), Apple Pay та Google Pay

  EMV

  Архітектура EMV складається з декількох ключових компонентів. Основою є чіп-карта, яка містить захищений мікропроцесор та операційну систему. На чіпі зберігаються криптографічні ключі, сертифікати та платіжні застосунки.

  1. Ініціалізація транзакції. Термінал визначає наявність чіпа на карті та встановлює з ним контакт. Відбувається обмін базовою інформацією між терміналом і картою.

  2. Вибір застосунку. Карта може містити кілька платіжних застосунків (наприклад, для дебетових та кредитних операцій). Термінал отримує список доступних застосунків та обирає відповідний для транзакції.

  3. Автентифікація карти. Використовуються два основні методи: статична автентифікація даних (SDA) та динамічна автентифікація даних (DDA). При SDA термінал перевіряє цифровий підпис статичних даних карти. DDA додатково генерує динамічний підпис для кожної транзакції, що забезпечує вищий рівень безпеки.

4. Верифікація власника карти. Вона може відбуватися через PIN-код (онлайн або офлайн), підпис, або комбінацію методів. Карта зберігає зашифрований PIN і може самостійно перевірити його правильність.

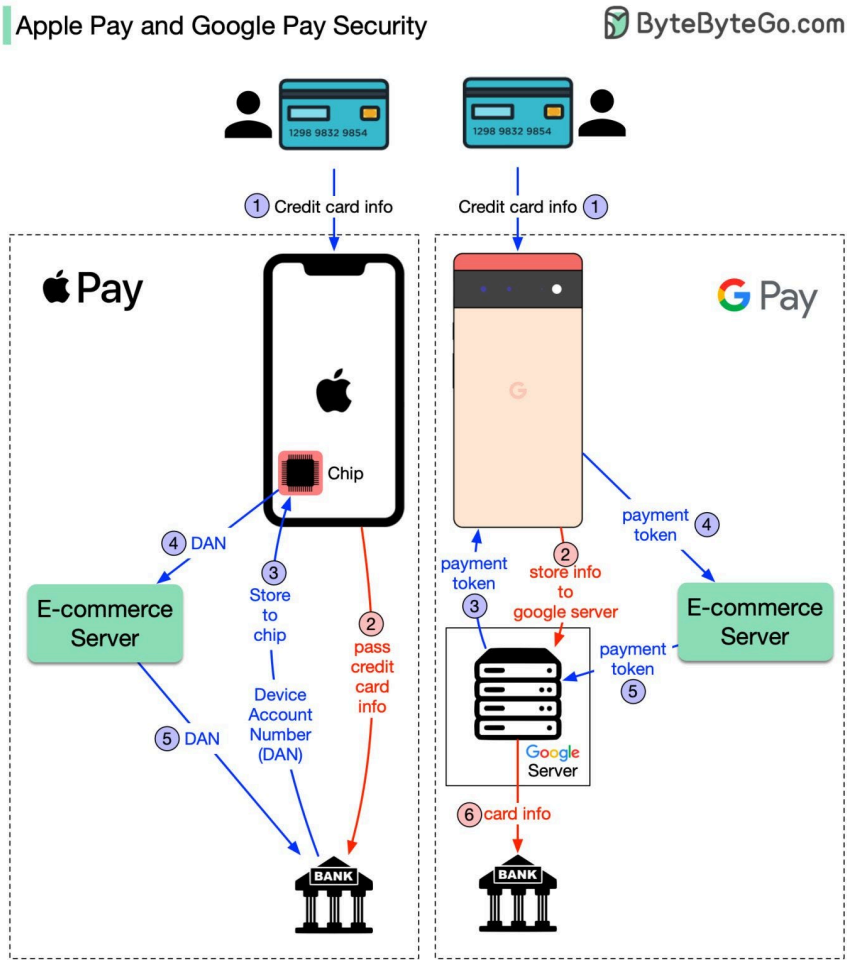
5. Аналіз ризиків транзакції. Термінал і карта оцінюють параметри операції (суму, частоту використання, локацію) та визначають необхідність онлайн-авторизації.

6. Криптограмна обробка. Карта генерує криптограму (ARQC - Authorization Request Cryptogram), яка містить деталі транзакції та результати попередніх перевірок. Ця криптограма відправляється банку-емітенту через термінал.

7. Онлайн-обробка. Банк-емітент перевіряє криптограму та приймає рішення щодо авторизації. У відповідь генерується криптограма ARPC (Authorization Response Cryptogram).

8. Завершення транзакції. Карта перевіряє відповідь банку та генерує фінальну криптограму (TC - Transaction Certificate або AAC - Application Authentication Cryptogram), яка підтверджує результат операції.

Apple Pay та Google Pay використовує специфікацію токенізації платежу EMV



2. **Загальні теоретичні відомості про побудову платіжних систем**
    - **Специфікація SET (Secure Electronic Transaction)**: опис концепції, стандартів та мети SET.

Специфікація SET (Secure Electronic Transaction) є протоколом безпеки для електронних платіжних карток, розробленим Visa та Mastercard для захисту онлайн-транзакцій. Розглянемо її детальну структуру та принципи роботи.

SET забезпечує конфіденційність інформації через унікальний механізм подвійного підпису, який дозволяє відокремити платіжну інформацію від деталей замовлення. Торговець отримує лише інформацію про замовлення, тоді як банк – тільки платіжні дані.

Основні учасники SET-транзакції:

1. Власник карти (покупець)
2. Торговець
3. Банк-емітент карти
4. Банк-еквайр торговця
5. Платіжний шлюз
6. Центр сертифікації

Процес SET-транзакції відбувається наступним чином:

Спочатку відбувається ініціалізація покупки. Покупець формує замовлення. Створює два блоки інформації: один з деталями замовлення, інший з платіжною інформацією.

Далі формується подвійний підпис. Система створює хеші обох блоків інформації, конкатенує їх та підписує приватним ключем покупця. Цей механізм забезпечує зв'язок між замовленням та платежем, не розкриваючи конфіденційні дані.

Наступним кроком є шифрування даних. Платіжна інформація шифрується публічним ключем банку, а інформація про замовлення – ключем торговця. Це гарантує, що кожна сторона отримає лише необхідні їй дані.

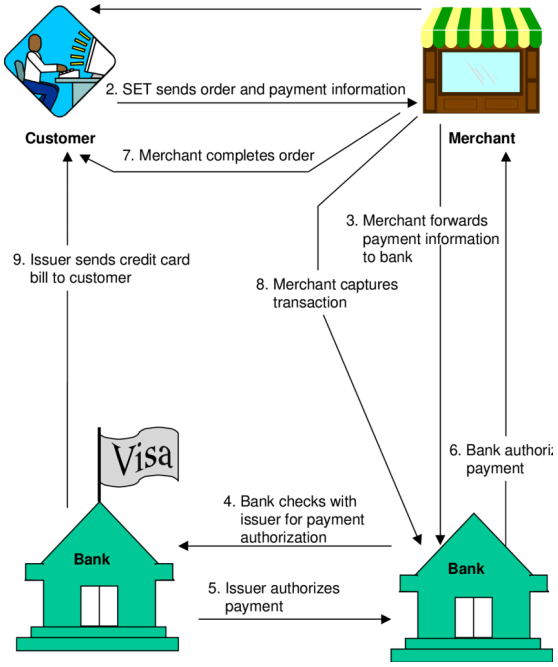
Торговець, отримавши запит, перевіряє подвійний підпис та інформацію про замовлення. Після цього він пересилає зашифровану платіжну інформацію до банку через платіжний шлюз.

Банк розшифровує платіжну інформацію своїм приватним ключем, перевіряє її достовірність та проводить авторизацію транзакції. Результат авторизації передається назад торговцю через платіжний шлюз.

Завершальним етапом є підтвердження транзакції. Торговець надсилає покупцю підтвердження замовлення, а банк – підтвердження платежу.

Безпека SET базується на: сертифікатах X.509 для автентифікації всіх учасників.

На сьогодні SET залишається важливим історичним прикладом комплексного підходу до безпеки електронних платежів, хоча в практичному використанні його замінили більш прості та економічні рішення.



- **Основні характеристики платіжних систем**:

Ключові вимоги до безпеки:

Конфіденційність в платіжних системах забезпечується через шифрування всіх критичних даних, включаючи персональні дані користувачів, деталі транзакцій та облікові дані. Використовуються сучасні криптографічні алгоритми та протоколи захищеного зв'язку. Особлива увага приділяється захисту даних платіжних карток згідно зі стандартом PCI DSS.

Цілісність даних досягається використанням цифрових підписів та хеш-функцій для кожної транзакції. Також застосовуються механізми контролю версій та журналювання всіх операцій. (**WAL**)

3. **Особливості платіжних систем для мікроплатежів**

Мікроплатежі - це фінансові транзакції на невеликі суми (зазвичай менше 10 доларів), які потребують спеціальних підходів до обробки через особливості економічної доцільності та технічної реалізації. Традиційні платіжні системи часто виявляються неефективними для обробки мікроплатежів через високі транзакційні витрати. У відповідь на цю проблему були розроблені спеціалізовані системи, серед яких особливу увагу заслуговують Payword та Micromint.

Система Payword

Принцип роботи з використанням ланцюга хешів

Payword базується на концепції криптографічного ланцюга хешів, де кожен елемент пов'язаний з попереднім через односторонню хеш-функцію. Система працює наступним чином:

1. **Генерація ланцюга хешів:**
    a. Користувач створює випадкове значення w_n
    b. Послідовно застосовує хеш-функцію для створення ланцюга: $w_{i-1} = H(w_i)$
    c. Формується послідовність: $w_0, w_1, w_2, ..., w_n$

Приклад

Припустимо, користувач хоче створити ланцюг довжиною n=100 для здійснення 100 мікроплатежів.

Далі відбувається послідовне хешування:

1. Беремо w_{100} (випадкове значення)
2. Застосовуємо хеш-функцію: $w_{99} = H(w_{100})$
3. Потім: $w_{98} = H(w_{99})$
4. І так далі до $w_0 = H(w_1)$

Кожне значення в ланцюгу можна представити як: $w_{i-1} = H(w_i)$, де i змінюється від n до 1

2. **Властивості ланцюга:**
    a. Однонаправленість:
    Знаючи w_{i-1}, неможливо обчислити w_i
    Це забезпечується властивостями криптографічної хеш-функції
    Наприклад, маючи w_5, неможливо отримати w_6

    b. Верифікованість:
    Можна легко перевірити, чи належить значення до ланцюга
    Для перевірки достатньо застосувати хеш-функцію і порівняти з попереднім значенням
    Наприклад, якщо у вас є w_5 і w_6, ви можете перевірити чи $w_5 = H(w_6)$

Етапи здійснення транзакцій

Процес налаштування:

- Користувач генерує ланцюг хешів
- Бере w_0 (перше значення ланцюга)
- Створює сертифікат, який включає:
    - Ідентифікатор користувача
    - w_0
    - Термін дії
    - Вартість одного токена
- Підписує сертифікат своїм цифровим підписом
- Надсилає сертифікат продавцю

Процес оплати:

- Для першого платежу надає w_1
- Для другого платежу надає w_2
- І так далі
- Продавець перевіряє кожне нове значення, застосовуючи хеш-функцію
- Якщо $H(w_i) = w_{i-1}$, платіж приймається

Механізми захисту

Аспект безпеки	Реалізація	Результат
Цілісність	Криптографічне хешування	Неможливість модифікації значень
Автентифікація	Цифровий підпис початкового значення	Підтвердження джерела платежів
Захист від подвійних витрат	Унікальність елементів ланцюга	Неможливість повторного використання токенів

Система Micromint

Принцип використання одноразових токенів

Micromint використовує концепцію цифрових монет, які генеруються через криптографічні механізми:

1. Базова концепція:

- Кожна монета це унікальний цифровий токен
- Токени генеруються централізовано емітентом (банком)
- Вартість створення токена навмисно зроблена високою
- Вартість перевірки токена навпаки - дуже низька

2. Особливості токенів:

- Токен представляє собою набір значень, які дають однакове значення при хешуванні
- Такі набори називаються k-way колізіями (k-кратними колізіями)
- Чим більше k, тим складніше згенерувати токен
- Чим більше k, тим простіше перевірити справжність токена

Процес генерування та використання токенів

Генерація токенів:

1. Підготовчий етап:
   - Емітент визначає параметри системи:
   - k (кількість значень для колізії)
   - Розмір вихідного значення хеш-функції
   - Кількість монет для випуску
   - Термін дії монет

2 . Процес мінтингу (створення монет):

- Генерація великої кількості випадкових значень
- Застосування до них криптографічної хеш-функції
- Пошук наборів з k значень, які дають однакове значення хешу
- Кожний такий набір стає одним токеном

Приклад створення токену (для k=4):

- Генеруємо мільйони випадкових значень
- Хешуємо кожне значення
- Шукаємо 4 різних значення x_1, x_2, x_3, x_4
- Для яких $H(x_1) = H(x_2) = H(x_3) = H(x_4)$
- Набір (x_1, x_2, x_3, x_4) стає токеном

Використання токенів:

1. Процес купівлі токенів:
- Користувач звертається до емітента
- Оплачує бажану кількість токенів
- Отримує токени через захищений канал

2. Здійснення платежу:
- Користувач передає токен продавцю
- Продавець перевіряє валідність:
  - Хешує всі значення з токену
  - Перевіряє, чи дають вони однакове значення
  - Перевіряє, чи не був токен використаний раніше
- При успішній перевірці товар/послуга надається

- Токен позначається як використаний

Система безпеки

Криптографічний контроль:

- Використання стійких хеш-функцій
- Механізм к-кратних колізій
- Централізована валідація

Економічна безпека:

- Висока вартість генерації токенів
- Низька вартість перевірки
- Одноразове використання

Характеристика	**Payword**	**Micromint**
Принцип роботи	Ланцюг хешів	Токени-колізії
Масштабованість	Висока	Середня
Вартість транзакції	Дуже низька	Низька
Складність впровадження	Середня	Висока
Централізованість	Частково централізована	Повністю централізована

4. **Протоколи електронних грошей**

Основні типи електронних грошей та їх характеристика

Онлайн моделі електронних грошей

Онлайн моделі електронних грошей характеризуються необхідністю постійного підключення до мережі для здійснення транзакцій.

Характеристики онлайн моделей:

- Необхідність прямого з'єднання з банком при кожній транзакції
- Висока безпека завдяки миттєвій верифікації
- Можливість блокування операцій в реальному часі
- Централізований контроль транзакцій

Переваги:

- Миттєва верифікація транзакцій
- Високий рівень безпеки
- Можливість відміни транзакцій
- Актуальний баланс в реальному часі

Недоліки:

- Залежність від інтернет-з'єднання
- Більші витрати на обробку транзакцій
- Можливі затримки при високому навантаженні
- Необхідність підтримки серверної інфраструктури

Офлайн моделі електронних грошей

Офлайн моделі дозволяють здійснювати транзакції без постійного підключення до мережі.

Характеристики офлайн моделей:

- Можливість здійснення транзакцій без підключення до мережі
- Зберігання коштів на локальному носії
- Відкладена верифікація транзакцій
- Децентралізований характер операцій

Переваги:

- Незалежність від підключення до мережі
- Нижча вартість транзакцій
- Швидкість проведення операцій
- Можливість роботи в умовах обмеженої connectivity

Недоліки:

- Підвищений ризик подвійних витрат
- Складніша система безпеки
- Обмежені можливості відміни транзакцій
- Потреба в спеціальних пристроях зберігання

Вимоги до протоколів електронних грошей

Захищеність від підробки: Захищеність від підробки є основоположною вимогою для будь-якої системи електронних грошей. Вона забезпечується комплексом технічних рішень та криптографічних методів. Кожна електронна грошова одиниця повинна мати унікальну ідентифікацію, яка неможлива для підробки або копіювання.

Для реалізації захисту від підробки використовуються криптографічні алгоритми високої складності. Кожна транзакція підписується цифровим підписом емітента, що гарантує її автентичність. Додатково застосовуються криптографічні хеш-функції для створення унікальних ідентифікаторів транзакцій та перевірки цілісності даних.

Важливим елементом захисту є багаторівнева система верифікації. На кожному етапі транзакції проводиться перевірка автентичності електронних грошей, їх походження та правомірності використання. Це включає перевірку цифрових підписів, валідацію унікальних ідентифікаторів та контроль цілісності даних.

Конфіденційність: Конфіденційність у системах електронних грошей забезпечує захист особистої інформації користувачів та деталей їхніх транзакцій. Це включає захист персональних даних, інформації про транзакції та метаданих, пов'язаних з фінансовими операціями.

Для забезпечення конфіденційності використовується наскрізне шифрування даних. Вся інформація, що передається між учасниками системи, шифрується з використанням сучасних криптографічних алгоритмів. Це гарантує, що дані залишаються захищеними навіть у разі перехоплення.

Системи електронних грошей також впроваджують суворий контроль доступу до інформації. Кожен учасник системи має доступ лише до тієї інформації, яка необхідна для виконання його функцій. Додатково застосовуються методи анонімізації даних, які дозволяють приховати зв'язок між конкретними транзакціями та особами.

Ідентифікація та анонімність транзакцій: Системи електронних грошей повинні забезпечувати баланс між можливістю ідентифікації користувачів для запобігання злочинній діяльності та збереженням їх приватності. Це досягається через впровадження гнучких механізмів ідентифікації та різних рівнів анонімності.

Ідентифікація користувачів зазвичай відбувається на етапі реєстрації в системі. При цьому використовуються різні методи верифікації особи, від простої електронної пошти до повної KYC (Know Your Customer) процедури. Рівень необхідної ідентифікації може залежати від суми транзакцій та вимог регуляторів.

Для забезпечення анонімності транзакцій використовуються методи псевдонімізації. Користувачам присвоюються унікальні ідентифікатори, які не розкривають їх реальної особистості. При цьому система зберігає можливість розкриття інформації про користувача у випадку правових вимог або підозри у незаконній діяльності.

Захищеність протоколів

Захист від повторного використання: Захист від повторного використання електронних грошей є критично важливим для запобігання подвійним витратам. У онлайн системах це забезпечується через централізований реєстр всіх транзакцій, який оновлюється в реальному часі.

Кожна транзакція отримує унікальний ідентифікатор та часову мітку. Система постійно перевіряє всі нові транзакції на предмет дублювання з

уже існуючими. У випадку виявлення спроби повторного використання коштів, транзакція блокується.

В офлайн системах захист від повторного використання реалізується через локальні журнали транзакцій та періодичну синхронізацію з центральною базою даних. Кожен термінал зберігає інформацію про проведені через нього транзакції та регулярно оновлює цю інформацію з центральною системою.

Шифрування: Шифрування в системах електронних грошей відбувається на кількох рівнях. На транспортному рівні використовуються протоколи TLS/SSL для захисту каналів передачі даних. Це забезпечує конфіденційність та цілісність інформації під час її передачі між учасниками системи.

На рівні даних застосовується шифрування самого вмісту транзакцій та персональної інформації користувачів. Використовуються сучасні алгоритми симетричного та асиметричного шифрування, що забезпечує надійний захист інформації.

Особлива увага приділяється захисту ключів шифрування. Використовуються спеціальні апаратні модулі безпеки (HSM) для зберігання критично важливих ключів. Впроваджуються процедури регулярної зміни ключів та їх резервного копіювання.

Використання цифрових підписів: Цифрові підписи є ключовим елементом безпеки в системах електронних грошей. Вони забезпечують автентифікацію учасників транзакцій та гарантують цілісність переданих даних. Кожна транзакція підписується відправником, що робить неможливим її підробку або модифікацію.

Процес використання цифрових підписів починається з генерації пари ключів - приватного та публічного. Приватний ключ зберігається користувачем у безпечному місці та використовується для підписання транзакцій. Публічний ключ доступний всім учасникам системи та використовується для перевірки підпису.

При здійсненні транзакції система перевіряє валідність цифрового підпису, що підтверджує автентичність відправника та цілісність даних. Це також

забезпечує неможливість відмови від транзакції, оскільки тільки власник приватного ключа міг створити дійсний підпис.

Зберігання підписаних даних відбувається в захищеному вигляді з використанням надійних систем резервного копіювання. Це забезпечує можливість аудиту транзакцій та вирішення спорів у майбутньому.

Характеристика	Онлайн Модель	Офлайн модель
Безпека	Вища	Середня
Швидкість транзакцій	Залежить від мережі	Висока
Вартість операцій	Вища	Нижча
Масштабованість	Обмежена	Висока
Зручність використання	Середня	Висока
Можливість відміни	Так	Обмежена
Анонімність	Обмежена	Висока

5. **Огляд та аналіз криптографічних механізмів систем WebMoney та PayPal**
    - У платіжній системі **WebMoney** реалізовано кілька рівнів захисту для забезпечення конфіденційності, автентифікації та цілісності даних, що допомагає уникнути атак та фальсифікації транзакцій.

➢ Криптографічний захист

Асиметричне шифрування (RSA). Використовується для безпечної передачі даних між клієнтами та серверами. RSA гарантує, що дані

шифруються відкритим ключем і можуть бути розшифровані лише власником закритого ключа, що захищає їх від несанкціонованого доступу.

Симетричне шифрування (AES). Застосовується для захищеного зберігання інформації на серверах WebMoney. Симетричне шифрування є менш ресурсомістким і забезпечує швидке шифрування та дешифрування даних користувача, зберігаючи їх конфіденційність і захищеність.

➢ Верифікація користувачів

Цифрові сертифікати видаються WebMoney для кожного користувача і є основою автентифікації. Кожен сертифікат містить інформацію про користувача, його публічний ключ і цифровий підпис, підтверджений WebMoney, що дозволяє системі впевнитися в ідентичності користувача.

Криптографічні підписи використовуються для підпису транзакцій. Ці підписи гарантують цілісність даних і дозволяють впевнитися, що транзакцію здійснив саме власник облікового запису.

➢ Ключові механізми безпеки

Шифрування даних гаманця. Конфіденційна інформація про гаманці, як-от баланс і дані транзакцій, захищена симетричним шифруванням, що гарантує збереження даних у захищеному вигляді.

Цифрові підписи для транзакцій. Для кожної транзакції WebMoney використовує цифрові підписи, які перевіряють автентичність транзакцій і цілісність переданих даних. Це захищає від підробок та шахрайства.

Автентифікація користувачів за допомогою сертифікатів. Кожен користувач має свій сертифікат, виданий WebMoney, який використовується для підтвердження його особи під час входу в систему та проведення фінансових операцій.

➢ Оцінка захищеності

Безпека проти атак типу "людина посередині" (Man-in-the-Middle). Асиметричне шифрування та цифрові підписи захищають від перехоплення та зміни даних сторонніми особами.

Захист від фальсифікації транзакцій. Цифрові підписи на кожній транзакції ускладнюють підробку даних, оскільки тільки користувач зі своїм закритим ключем може підписати транзакцію.

Контроль доступу за допомогою токенів та цифрових підписів. WebMoney застосовує токени доступу та криптографічні підписи для авторизації користувачів та контролю доступу до гаманців, що підвищує загальну безпеку платформи.

Завдяки використанню асиметричного та симетричного шифрування, цифрових сертифікатів, підписів та токенів WebMoney забезпечує високий рівень безпеки для даних та транзакцій. Криптографічні механізми ефективно захищають від поширених атак і забезпечують конфіденційність та автентичність транзакцій, роблячи WebMoney надійною платформою для електронних платежів.

- У платіжній системі **PayPal** реалізовано сучасні криптографічні технології та багаторівневі заходи безпеки для захисту конфіденційності, автентифікації та цілісності даних користувачів.

➢ Використання SSL/TLS

PayPal використовує **SSL/TLS** для захищеного з'єднання між клієнтом і сервером, що забезпечує конфіденційність переданих даних. Ці протоколи шифрують дані між браузером користувача та серверами PayPal, запобігаючи їх перехопленню третіми сторонами.

Реалізація TLS гарантує, що всі дані користувачів, як-от облікові дані або фінансова інформація, залишаються приватними й доступні лише автентифікованим сторонам.

➢ Шифрування на стороні клієнта та автентифікація

Шифрування на стороні клієнта. Клієнтське шифрування захищає дані ще до їх відправлення на сервер. Це особливо важливо для захисту

конфіденційної інформації, яка може передаватися через браузери або мобільні додатки.

OAuth 2.0 і токени доступу. PayPal використовує протокол OAuth 2.0 для автентифікації та авторизації. Це дозволяє користувачам безпечно авторизуватись у додатках та сервісах, не розкриваючи свої паролі. Токени доступу дозволяють надавати обмежений доступ до облікового запису користувача, що знижує ризик витоку пароля.

Токенізація. Токени доступу генеруються для авторизації та мають обмежений термін дії, що дозволяє додатково захистити інформацію від перехоплення.

➢ Підтримка багаторівневої автентифікації (2FA) та запобігання шахрайству

Багаторівнева автентифікація (2FA). PayPal підтримує двофакторну автентифікацію, яка вимагає введення додаткового коду, що надсилається користувачу через SMS або спеціальний мобільний додаток. Це забезпечує додатковий рівень захисту при доступі до облікового запису.

Запобігання шахрайству за допомогою машинного навчання. PayPal використовує алгоритми машинного навчання для виявлення аномальної активності, такої як підозрілі спроби входу або незвичні транзакції. Система автоматично ідентифікує потенційно шахрайські дії та може обмежити або зупинити транзакцію, якщо виявлені ризики.

➢ Оцінка захищеності

Високий рівень безпеки від підробок та перехоплення. Використання SSL/TLS забезпечує захист від перехоплення даних (типу "людина посередині"), а двофакторна автентифікація зменшує ризик несанкціонованого доступу.

Підтримка сучасних криптографічних стандартів. PayPal регулярно оновлює свої алгоритми шифрування і автентифікації відповідно до

сучасних стандартів безпеки, що робить її стійкою до більшості відомих атак і забезпечує надійний захист даних користувачів.

Системи захисту від шахрайства. Завдяки аналітиці і машинному навчанню, PayPal має надійну систему моніторингу транзакцій, яка в реальному часі аналізує ризики та відсікає підозрілі дії, що забезпечує додатковий рівень безпеки.

Поєднання SSL/TLS, шифрування на стороні клієнта, OAuth 2.0, двофакторної автентифікації та машинного навчання робить PayPal одним із найбільш захищених платіжних сервісів. Використання сучасних криптографічних стандартів і алгоритмів запобігає основним загрозам, таким як перехоплення даних, фальсифікація транзакцій і несанкціонований доступ.

6. **Порівняльний аналіз WebMoney та PayPal з точки зору захищеності та вибору криптографічних примітивів**

Обидві системи, **WebMoney** та **PayPal**, застосовують різні криптографічні примітиви та методи захисту для забезпечення конфіденційності, автентифікації, контролю доступу та цілісності даних користувачів. Однак вони відрізняються підходами до шифрування, автентифікації та захисту даних.

Характеристика	**WebMoney**	**PayPal**
Конфіденційність	Асиметричне шифрування (RSA) для передачі даних, симетричне (AES) для зберігання	SSL/TLS для з'єднання, шифрування на стороні клієнта

Автентифікація	Цифрові сертифікати, криптографічні підписи	OAuth 2.0, токени доступу, 2FA
Контроль доступу	Сертифікати користувачів і токени	Токени OAuth і 2FA
Захист від атак	Захист від атак типу "людина посередині", цифрові підписи	Захист від атак "людина посередині", машинне навчання для запобігання шахрайству
Запобігання шахрайству	Цифрові підписи та сертифікати	Аналіз поведінки з машинним навчанням
Сучасні криптоалгоритми	AES для зберігання, RSA для передачі даних	AES, RSA, HMAC, TLS

Переваги та недоліки використання різних криптографічних підходів

Криптографічний підхід	Переваги	Недоліки
Асиметричне шифрування (RSA)	Забезпечує високий рівень безпеки, використовується для автентифікації та шифрування даних під час передачі.	Ресурсомісткий, не підходить для великої кількості одночасних запитів.

Симетричне шифрування (AES)	Висока ефективність, підходить для зберігання даних у зашифрованому вигляді.	Потребує безпечного зберігання ключів, підходить для закритих систем.
SSL/TLS	Захищає канали зв'язку, забезпечуючи конфіденційність і цілісність даних під час передачі.	Вразливий до атак типу "людина посередині" у разі поганої реалізації.
OAuth 2.0 з токенами	Спрощує управління доступом, дозволяє використовувати токени замість паролів.	Потребує надійного управління токенами для запобігання крадіжкам.
Двофакторна автентифікація (2FA)	Додатковий рівень захисту, що зменшує ймовірність несанкціонованого доступу.	Може бути незручним для користувачів, потребує додаткових пристроїв або методів.
Машинне навчання	Динамічний захист від шахрайства, аналізуючи поведінкові фактори.	Потребує обробки великих обсягів даних, може мати помилкові спрацювання.

7. **Висновки**

WebMoney і **PayPal** обидві мають високий рівень захищеності, але використовують різні підходи до криптографічного захисту та управління доступом.

- **WebMoney** фокусується на використанні цифрових сертифікатів і асиметричного шифрування для автентифікації користувачів, що робить її придатною для середовищ з підвищеними вимогами до автентифікації та захисту. Комбінація RSA для передачі даних та AES для їхнього зберігання забезпечує високий рівень безпеки, але така система може бути менш зручною для користувачів через складність налаштувань сертифікатів.
- **PayPal** пропонує більш гнучкий підхід, використовуючи протоколи OAuth 2.0, SSL/TLS і двофакторну автентифікацію, що підходить для глобального ринку. Це забезпечує ефективний контроль доступу та конфіденційність даних під час передачі. Крім того, використання алгоритмів машинного навчання для захисту від шахрайства дозволяє динамічно ідентифікувати потенційно небезпечні дії, що підвищує безпеку системи.

Рекомендації щодо покращення захисту електронних платіжних систем

- **Постійне оновлення криптографічних алгоритмів.** З огляду на постійний розвиток технологій зламу, рекомендується регулярно оновлювати криптографічні алгоритми, такі як перехід з RSA на більш сучасні алгоритми (наприклад, ECC – Elliptic Curve Cryptography), які є менш ресурсомісткими та забезпечують такий же рівень безпеки.
- **Розширення використання машинного навчання для виявлення аномалій.** PayPal ефективно використовує машинне навчання для запобігання шахрайству, і цей підхід може бути застосований також у WebMoney. Алгоритми машинного навчання можуть ідентифікувати нетипову поведінку користувачів і блокувати підозрілі дії, що підвищує загальну захищеність системи
- **Розширення багаторівневої автентифікації.** Додавання двофакторної автентифікації до WebMoney могло б підвищити рівень безпеки облікових записів і зменшити ризик несанкціонованого

доступу. Додаткові фактори автентифікації, як-от SMS або мобільний додаток для підтвердження входу, стали б корисним доповненням.

- **Вдосконалення управління токенами**. PayPal і WebMoney можуть вдосконалити управління токенами доступу, наприклад, шляхом обмеження часу дії токенів або впровадження політик оновлення токенів, щоб зменшити ризик їх компрометації.
- **Запровадження проактивних тестувань на уразливості.** Регулярні тестування безпеки та аналіз потенційних уразливостей можуть допомогти виявити слабкі місця в системах WebMoney і PayPal до того, як вони стануть об'єктами атак. Це можуть бути тестування на проникнення, аналіз коду та стрес-тестування.
- **Освіта користувачів щодо безпечного використання платіжних систем.** Рекомендації для користувачів щодо налаштування надійних паролів, використання 2FA, безпечного зберігання сертифікатів (для WebMoney) та регулярного моніторингу активності в обліковому записі можуть знизити ризики шахрайства і підвищити загальний рівень безпеки систем.

Ретельне використання сучасних криптографічних протоколів, таких як TLS, AES, OAuth 2.0, і багаторівнева автентифікація забезпечують високий рівень захищеності в платіжних системах WebMoney та PayPal. Подальше вдосконалення, зокрема через впровадження машинного навчання, управління токенами, розширення багаторівневої автентифікації та освіту користувачів, допоможе обом платформам залишатися надійними та захищеними на ринку електронних платежів.